CLAIMS

What is claimed is:

1. A method for predicting fraudulent identification usage, comprising:

detecting a context for a use of an identification via a communication line at a fraud protection service;

analyzing said context for use of said identification in view of a plurality of entries for use of said identification; and

specifying a level of suspicion of fraudulent use of said identification according to said analysis of said context.

2. The method for predicting fraudulent identification usage according to claim 1, wherein said identification comprises at least one from among a caller identity, an account number, a service number, and a password.

3. The method for predicting fraudulent identification usage according to claim 1, wherein said context is detected from a context inference service executing with a trusted telephone network.

4. The method for predicting fraudulent identification usage according to claim 1, wherein said context is detected from a context inference service executing outside a trusted telephone network.

5. The method for predicting fraudulent identification usage according to claim 1, wherein said context comprises at least one

from among an identity of a caller, an identity of a callee, a device utilized by said caller, a device utilized by said callee, an inferred location of said caller, a scheduled location of said caller, an inferred location of said callee, a scheduled location of said callee, an on behalf of party, a billing plan, an order placed, a service requested for access, and a subject.

6. The method for predicting fraudulent identification usage according to claim 5, wherein said inferred location of said caller and said callee further comprises a global positioning system location, a street address, a geographical area, a business location, and a home location.

7. The method for predicting fraudulent identification usage according to claim 1, wherein said billing plan further comprises at least one from among a service provider, an account provider and at least one shipping address.

8. The method for predicting fraudulent identification usage according to claim 1, wherein said use of said identification comprises at least one from among accessing a service from a service provider identified by said identification and placing an order with payment to an account provider identified by said identification.

9. The method for predicting fraudulent identification usage according to claim 1, wherein said identification is utilized for an in-store purchase.

10. The method for predicting fraudulent identification usage according to claim 1, wherein said identification is utilized to identify a caller to a call.

11. The method for predicting fraudulent identification usage

according to claim 1, wherein said identification is utilized to access a web based service.

12. The method for predicting fraudulent identification usage according to claim 1, wherein said identification is utilized for a telephone purchase.

13. The method for predicting fraudulent identification usage according to claim 1, wherein said identification is utilized for a web merchant purchase.

14. The method for predicting fraudulent identification usage according to claim 1, wherein analyzing said context for use of said identification further comprises:

analyzing said context in view of a fraud value associated with said context.

15. The method for predicting fraudulent identification usage according to claim 1, wherein analyzing said context for use of said identification further comprises:

accessing a schedule of events associated with said identification; and

comparing a location for origination of use of said identification in said context with said schedule of events.

16. The method for predicting fraudulent identification usage according to claim 1, further comprising:

responding to said level of suspicion according to a preference designated by a provider included in said context.

17. The method for predicting fraudulent identification usage according to claim 1, further comprising:

responding to said level of suspicion according to a preference designated by an owner of said identification.

18. The method for predicting fraudulent identification usage according to claim 1, further comprising:

controlling access to additional authentication of said identification.

19. A system for predicting fraudulent identification usage, comprising:

a fraud protection service server communicatively connected to a trusted telephone network;

means for detecting a context for a use of an identification via a communication line at said fraud protection service server;

means for analyzing said context for use of said identification in view of a plurality of entries for use of said identification; and

means for specifying a level of suspicion of fraudulent use of said identification according to said analysis of said context.

20. The system for predicting fraudulent identification usage according to claim 19, wherein said identification comprises at least one from among a caller identity, an account number, a service number, and a password.

21. The system for predicting fraudulent identification usage according to claim 19, wherein said context is detected from a context inference service executing with said trusted telephone network.

22. The system for predicting fraudulent identification usage according to claim 19, wherein said context is detected from a context inference service executing outside said trusted telephone network.

23. The system for predicting fraudulent identification usage according to claim 19, wherein said context comprises at least one from among an identity of a caller, an identity of a callee, a device utilized by said caller, a device utilized by said callee, an inferred location of said caller, a scheduled location of said caller, an inferred location of said callee, a scheduled location of said callee, an on behalf of party, a billing plan, an order placed, a service requested for access, and a subject.

24. The system for predicting fraudulent identification usage according to claim 5, wherein said inferred location of said caller and said callee further comprises a global positioning system location, a street address, a geographical area, a business location, and a home location.

25. The system for predicting fraudulent identification usage according to claim 19, wherein said billing plan further comprises at least one from among a service provider, an account provider and at least one shipping address.

26. The system for predicting fraudulent identification usage according to claim 19, wherein said use of said identification comprises at least one from among accessing a service from a

service provider identified by said identification and placing an order with payment to an account provider identified by said identification.

27. The system for predicting fraudulent identification usage according to claim 19, wherein said identification is utilized for an in-store purchase.

28. The system for predicting fraudulent identification usage according to claim 19, wherein said identification is utilized to identify a caller to a call.

29. The system for predicting fraudulent identification usage according to claim 19, wherein said identification is utilized to access a web based service.

30. The system for predicting fraudulent identification usage according to claim 19, wherein said identification is utilized for a telephone purchase.

31. The system for predicting fraudulent identification usage according to claim 19, wherein said identification is utilized for a web merchant purchase.

32. The system for predicting fraudulent identification usage according to claim 19, wherein said means for analyzing said context for use of said identification further comprises:

means for analyzing said context in view of a fraud value associated with said context.

33. The system for predicting fraudulent identification usage according to claim 19, wherein said means for analyzing said context for use of said identification further comprises:

means for accessing a schedule of events associated with said identification; and

means for comparing a location for origination of use of said identification in said context with said schedule of events.

34. The system for predicting fraudulent identification usage according to claim 19, further comprising:

means for responding to said level of suspicion according to a preference designated by a provider included in said context.

35. The system for predicting fraudulent identification usage according to claim 19, further comprising:

means for responding to said level of suspicion according to a preference designated by an owner of said identification.

36. The system for predicting fraudulent identification usage according to claim 19, further comprising:

means for controlling access to additional authentication of said identification.

37. A computer program product for predicting fraudulent identification usage, comprising:

a recording medium;

means, recorded on said recording medium, for detecting a context for a use of an identification via a communication line;

means, recorded on said recording medium, for analyzing said context for use of said identification in view of a plurality of entries for use of said identification; and

means, recorded on said recording medium, for specifying a level of suspicion of fraudulent use of said identification according to said analysis of said context.

38. The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for analyzing said context in view of a fraud value associated with said context.

39. The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for accessing a schedule of events associated with said identification; and

means, recorded on said recording medium, for comparing a location for origination of use of said identification in said context with said schedule of events.

40. The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for responding to said level of suspicion according to a preference designated by a provider included in said context.

41. The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for responding to said level of suspicion according to a preference designated by an owner of said identification.

42. The computer program product for predicting fraudulent identification usage according to claim 37, further comprising:

means, recorded on said recording medium, for controlling access to additional authentication of said identification.

43. A method for protecting an identification, comprising:

detecting a context for a use of an identification via a communication line at a fraud protection service; and

responsive to assigning a particular level of suspicion of fraudulent use to said use of said identification, requiring additional authentication for said use of said identification.

44. A method for protecting an identification from fraudulent usage, comprising:

detecting a context for a use of an identification via a communication line at a fraud protection service; and

responsive to assigning a particular level of suspicion of fraudulent use to said use of said identification, processing a decoy usage of said identification.

45. A method for protecting credit card account usage, comprising:

detecting a location for a request for a charge to a credit card account via a communication line at a fraud protection

service; and

comparing said location with a recent location detected for a individual associated with said credit card account; and

responsive to detecting infeasibility of presence by said individual at said location and said recent location within a measured lapsed period of time, only allowing said charge to said credit card if additional authentication by said individual is provided.

46. The method for protecting credit card account usage according to claim 45, wherein said location for said request for said charge is detected according to a line number associated with a device transmitting a credit card account number.

47. The method for protecting credit card account usage according to claim 45, wherein said recent location detected for said individual comprises a location detected for usage of a telephony device.

48. The method for protecting credit card account usage according to claim 45, wherein said recent location detected for said individual comprises a location detected for access to a network.

49. The method for protecting credit card account usage according to claim 45, wherein said recent location detected for said individual comprises a location of a store from which said credit card account is utilized to make a purchase.

50. The method for protecting credit card account usage according to claim 45, wherein said additional authentication of said individual is provided by voice authentication.

51. The method for protecting credit card account usage according to claim 45, further comprising:

responsive to detecting a particular level of infeasibility of presence by said individual at said location and said recent location within a measured lapsed period of time, disallowing said charge to said credit card.

52. A system for protecting credit card account usage, comprising:

a fraud protection service server communicatively connected to a network;

means for detecting a location for a request for a charge to a credit card account via a communication line at said fraud protection service server; and

means for comparing said location with a recent location detected for a individual associated with said credit card account; and

means responsive to detecting infeasibility of presence by said individual at said location and said recent location within a measured lapsed period of time, for only allowing said charge to said credit card if additional authentication by said individual is provided.

53. The system for protecting credit card account usage according to claim 52, wherein said location for said request for said charge is detected according to a line number associated with a device transmitting a credit card account number.

54. The system for protecting credit card account usage according to claim 52, wherein said recent location detected for said individual comprises a location detected for usage of a telephony device.

55. The system for protecting credit card account usage according to claim 52, wherein said recent location detected for said individual comprises a location detected for access to said network.

56. The system for protecting credit card account usage according to claim 52, wherein said recent location detected for said individual comprises a location of a store from which said credit card account is utilized to make a purchase.

57. The system for protecting credit card account usage according to claim 52, wherein said additional authentication of said individual is provided by voice authentication.

58. The system for protecting credit card account usage according to claim 52, further comprising:

means responsive to detecting a particular level of infeasibility of presence by said individual at said location and said recent location within a measured lapsed period of time, for disallowing said charge to said credit card.

59. A computer program product for protecting credit card account usage, comprising:

a recording medium;

means, recorded on said recording medium, for detecting a location for a request for a charge to a credit card account via

a communication line; and

means, recorded on said recording medium, for comparing said location with a recent location detected for a individual associated with said credit card account; and

means, recorded on said recording medium, for only allowing said charge to said credit card if additional authentication by said individual is provided where said presence of said individual at said location is detected to be infeasible.